IN THE CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method of encrypting and decrypting information, comprising:

(a) providing ~~information and~~ a key;[[,]]

(b) using said key to [[help]] construct a state generator and a sequence of permutations;[[,]]

(c) constructing a sequence of states with said state generator;[[,]] ~~and~~

(d) permuting said information with said sequence of permutations;[[,]]

(e~~d~~) encrypting said permuted information with said sequence of states to generate a ciphertext ~~if the permuted information is a message~~; and

(f) decrypting said ciphertext ~~information~~ with said sequence of states ~~if the permuted information is ciphertext~~.

2. (Currently Amended) The method of claim 1, further comprising providing ~~wherein~~ a perturbator operable to change ~~changes~~ a permutation in the construction of ~~to help generate~~ said sequence of permutations.

3. (Original) The method of claim 1 wherein said method is used in a consumer product.

4. (Original) The method of claim 1 wherein said method is used in a wireless application.

5. (Currently Amended) The method of claim 1, wherein steps (e) and (f) ~~in (d) encrypting and decrypting~~ use a function selected from the group consisting

of ~~one of the following functions:~~ an exclusive-or function, an addition modulo **L** function, a subtraction modulo **L** function, or a permutation function

6. (Original) The method of claim 1 wherein said state generator is a dynamical system.

7. (Original) The method of claim 6 wherein said dynamical system is iterative.

8. (Original) The method of claim 6 wherein said dynamical system is non-iterative.

9. (Original) The method of claim 6 wherein said dynamical system is non-autonomous.

10. (Original) The method of claim 6 wherein a matrix is used to generate said dynamical system.

11. (Original) The method of claim 10 wherein said matrix is changed with a perturbator.

12. (Original) The method of claim 11 wherein said perturbator uses a zero repeller.

13. (Original) The method of claim 6 wherein one or more permutations are used to generate said dynamical system.

14. (Currently Amended) The method of claim 13, wherein said one or more permutations~~, that generate said dynamical system, create~~ construct said sequence of states.

15. (Currently Amended) The method of claim 13, wherein said one or more permutations are changed with a perturbator.

16. (Original) The method of claim 6 wherein said dynamical system is changed with a perturbator

17. (Original) The method of claim 16 wherein said perturbator is implemented with a dynamical system.

18. (Currently Amended) A method of encrypting and decrypting information, comprising:

(a) providing ~~information and~~ a key;[[,]]

(b) using said key to [[help]] construct a state generator and a sequence of permutations;[[,]]

(c) constructing a sequence of states with said state generator;[[,]]

(d) permuting said sequence of states with said sequence of permutations;[[,]]

(e) encrypting said information with the permuted sequence of states to generate a ciphertext; ~~if said information is a message~~ and

(f) decrypting said ciphertext ~~information~~ with the permuted sequence of states ~~if said information is ciphertext~~.

19. (Currently Amended) The method of claim 18, further comprising providing ~~wherein~~ a perturbator operable to change ~~changes~~ a permutation in the construction of ~~to help generate~~ said sequence of permutations.

20. (Original) The method of claim 18 wherein said method is used in a consumer product.

21. (Original) The method of claim 18 wherein said method is used in a wireless application.

22. (Currently Amended) The method of claim 18, wherein steps (e) and (f) ~~in (e) encrypting and decrypting~~ use a function selected from the group consisting of ~~one of the following functions:~~ an exclusive-or function, an addition modulo **L** function, a subtraction modulo **L** function, or a permutation function.

23. (Original) The method of claim 18 wherein said state generator is a dynamical system.

24. (Original) The method of claim 23 wherein said dynamical system is iterative.

25. (Original) The method of claim 23 wherein said dynamical system is non-iterative.

26. (Original) The method of claim 23 wherein said dynamical system is non-autonomous.

27. (Original) The method of claim 23 wherein a matrix is used to generate said dynamical system.

28. (Original) The method of claim 27 wherein said matrix is changed with a perturbator.

29. (Original) The method of claim 28 wherein said perturbator uses a zero repeller.

30. (Original) The method of claim 23 wherein one or more permutations are used to generate said dynamical system.

31. (Currently Amended) The method of claim 30, wherein said one or more permutations construct ~~, that generate said dynamical system, create~~ said sequence of states.

32. (Currently Amended) The method of claim 30, wherein said one or more permutations are changed with a perturbator.

33. (Original) The method of claim 23 wherein said dynamical system is changed with a perturbator.

34. (Original) The method of claim 33 wherein said perturbator is implemented with a dynamical system.

35. (Currently Amended) A cryptographic machine, comprising:

(a) information;[[,]]

(b) a sequence of permutations~~, which permutes~~ for permuting said information;[[,]]

(c) a state generator~~, which constructs~~ for constructing a sequence of states;[[,]]

(d) a key~~, which determines~~ for determining said sequence of permutations and said state generator;[[.]] and

(e) a processor operable to encrypt said permuted information into a ciphertext using said sequence of states and to decrypt said ciphertext using said sequence of states ~~whereby if the permuted information is a permuted message, then said sequence of states encrypts said permuted message and if the permuted information is permuted ciphertext then said sequence of states decrypts said permuted ciphertext~~.

36. (Currently Amended) The machine of claim 35, further comprising ~~wherein~~ a perturbator operable to change ~~changes~~ a permutation in the construction of ~~to help generate~~ said sequence of permutations.

37. (Original) The machine of claim 35 wherein said machine runs in a consumer product.

38. (Original) The machine of claim 35 wherein said machine runs in a wireless application.

39. (Currently Amended) The machine of claim 35, wherein the ~~encryption and decryption use~~ processor uses a function selected from the group consisting of ~~one of the following functions:~~ an exclusive-or function, an addition modulo **L** function, a subtraction modulo **L** function, or a permutation function.

40. (Original) The machine of claim 35 wherein said state generator is a dynamical system.

41. (Original) The machine of claim 40 wherein said dynamical system is iterative.

42. (Original) The machine of claim 40 wherein said dynamical system is non-iterative.

43. (Original) The machine of claim 40 wherein said dynamical system is non-autonomous.

44. (Original) The machine of claim 40 wherein a matrix is used to generate said dynamical system.

45. (Original) The machine of claim 44 wherein said matrix is changed with a perturbator.

46. (Original) The machine of claim 45 wherein said perturbator uses a zero repeller.

47. (Original) The machine of claim 40 wherein one or more permutations are used to generate said dynamical system.

48. (Currently Amended) The machine of claim 47, wherein said one or more permutations~~, that generate said dynamical system, create~~ construct said sequence of states.

49. (Currently Amended) The machine of claim 47, wherein said one or more permutations are changed with a perturbator.

50. (Original) The machine of claim 40 wherein said dynamical system is changed with a perturbator.

51. (Original) The machine of claim 50 wherein said perturbator is implemented with a dynamical system.

52. (Currently Amended) A cryptography machine, comprising:

(a) information;

(b) a state generator~~, which constructs~~ for constructing a sequence of states;[[,]]

(c) a sequence of permutations~~, which permutes~~ for permuting said sequence of states;[[,]]

(d) a key~~, which determines~~ for determining said state generator and said sequence of permutations;[[,]] and

(e) a processor operable to encrypt said information into a ciphertext using the permuted sequence of states and to decrypt said ciphertext using said permuted sequence of states ~~whereby if said information is a message, then the permuted sequence of states encrypts said message and if said information is ciphertext then the permuted sequence of states decrypts said ciphertext~~.

53. (Currently Amended) The machine of claim 52, further comprising ~~wherein~~ a perturbator operable to change ~~changes~~ a permutation in the construction of ~~to help generate~~ said sequence of permutations

54. (Original) The machine of claim 52 wherein said machine runs in a consumer product.

55. (Original) The machine of claim 52 wherein said machine runs in a wireless application.

56. (Currently Amended) The machine of claim 52, wherein the ~~encryption and decryption use one of the following functions:~~ processor uses a function selected from the group consisting of an exclusive-or function, an addition modulo **L** function, a subtraction modulo **L** function, or a permutation function.

57. (Original) The machine of claim 52 wherein said state generator is a dynamical system.

58. (Original) The machine of claim 57 wherein said dynamical system is iterative.

59. (Original) The machine of claim 57 wherein said dynamical system is non-iterative.

60. (Original) The machine of claim 57 wherein said dynamical system is non-autonomous.

61. (Original) The machine of claim 57 wherein a matrix is used to generate said dynamical system.

62. (Original) The machine of claim 61 wherein said matrix is changed with a perturbator.

63. (Original) The machine of claim 62 wherein said perturbator uses a zero repeller.

64. (Original) The machine of claim 57 wherein one or more permutations are used to generate said dynamical system.

65. (Currently Amended) The machine of claim 64, wherein said one or more permutations construct ~~, that generate said dynamical system, create~~ said sequence of states.

66. (Currently Amended) The machine of claim 64, wherein said one or more permutations are changed with a perturbator.

67. (Original) The machine of claim 57 wherein said dynamical system is changed with a perturbator.

68. (Original) The machine of claim 67 wherein said perturbator is implemented with a dynamical system.

69. (Currently Amended) A cryptographic machine, comprising:

(a) information;

(b) at least one ~~or more~~ non-autonomous dynamical system ~~systems~~ for generating ~~, which generate~~ a sequence of states;[[,]]

(c) a key for determining ~~which determines~~ each said at least one non-autonomous dynamical system; and

(d) a processor operable to encrypt said information into a ciphertext using the generated sequence of states and to decrypt said ciphertext using said generated sequence of states ~~whereby if said information is a~~

~~message, then said machine encrypts said message using the states of one or more of said non-autonomous dynamical systems and if said information is ciphertext, then machine decrypts said ciphertext using the states of one or more of said non-autonomous dynamical systems~~.

70. (Currently Amended) The machine of claim 69, wherein each said at least one non-autonomous dynamical system is implemented with a distinct sequence of permutations.

71. (Original) The machine of claim 69 wherein each said sequence of permutations is implemented using a perturbator.

72. (Currently Amended) The machine of claim 69, wherein said machine ~~method~~ is used in a consumer product.

73. (Currently Amended) A method of encrypting and decrypting information, comprising:

(a) providing ~~information and~~ a key;[[,]]

(b) using said key to ~~help~~ construct a sequence of permutations;[[,]]

(c) encrypting said information into a ciphertext with said sequence of permutations; ~~if said information is a message~~ and

(d) decrypting said ciphertext with said sequence of permutations ~~if said information is ciphertext~~.

74. (Currently Amended) The method of claim 73, further comprising ~~wherein~~ a perturbator operable to change ~~changes~~ a permutation in the construction of ~~to help generate~~ said sequence of permutations

75. (Original) The method of claim 73 wherein said method is used in a wireless application.

76. (Original) The method of claim 73 wherein said method is used in a consumer product.

77. (Currently Amended) A method of generating random numbers, comprising:

(a) providing a state generator and a sequence of permutations;[[,]]

(b) generating a sequence of states with said state generator;[[,]]

(c) permuting said sequence of states with said sequence of permutations;[[,]] and

(d) extracting random numbers from the permuted sequence of states.

78. (Original) The method of claim 77 wherein said random numbers are used as encryption and decryption keys.